10-2-00

A

JC915 U.S. PTO 09/29/00

jc882 U.S. PTO 09/675530 09/29/00

Please type a plus sign (+) inside this box → [+]

PTO/SB/05 (4/98)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))

Attorney Docket No.	1662-28400 (P99-2550)
First Inventor or Application Identifier	Michael F. ANGELO et al.
Title	Fingerprint Verification Method Having Band Detection
Express Mail Label No.	EL705960689US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. [✔] * Fee Transmittal Form (e.g., PTO/SB/17) (Submit an original and a duplicate for fee processing)
2. [✔] Specification [Total Pages 18] (preferred arrangement set forth below) (plus cover sheet)
   - Descriptive title of the Invention
   - Cross References to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to Microfiche Appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings (if filed)
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
3. [✔] Drawing(s) (35 U.S.C. 113) [Total Sheets 4]
4. Oath or Declaration [Total Pages]
   - a. [ ] Newly executed (original or copy)
   - b. [ ] Copy from a prior application (37 C.F.R. § 1.63(d)) (for continuation/divisional with Box 16 completed)
     - i. [ ] DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).

NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).

5. [ ] Microfiche Computer Program (Appendix)
6. Nucleotide and/or Amino Acid Sequence Submission (if applicable, all necessary)
   - a. [ ] Computer Readable Copy
   - b. [ ] Paper Copy (identical to computer copy)
   - c. [ ] Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. [ ] Assignment Papers (cover sheet & document(s))
8. [ ] 37 C.F.R.§3.73(b) Statement (when there is an assignee) [ ] Power of Attorney
9. [ ] English Translation Document (if applicable)
10. [ ] Information Disclosure Statement (IDS)/PTO-1449 [ ] Copies of IDS Citations
11. [ ] Preliminary Amendment
12. [✔] Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
13. [ ] * Small Entity Statement(s) (PTO/SB/09-12) [ ] Statement filed in prior application, Status still proper and desired
14. [ ] Certified Copy of Priority Document(s) (if foreign priority is claimed)
15. [ ] Other: ....

16. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment:

[ ] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No: ______/______

Prior application information: Examiner ______ Group / Art Unit: ______

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

[ ] Customer Number or Bar Code Label 23505 (Insert Customer No. or Attach bar code label here) or [✔] Correspondence address below

Name	Jonathan M. Harris				
	Conley, Rose & Tayon, P.C.				
Address	PO Box 3267				
City	Houston	State	TX	Zip Code	77253-3267
Country	USA	Telephone	713-238-8000	Fax	713-238-8008

Name (Print/Type)	Marcella D. Watkins	Registration No. (Attorney/Agent)	36,962
Signature	Marcella D. Watkins	Date	September 29, 2000

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to send to this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

M:\C\1662\28400\PTO TRANS 01

Express Mail Label No. EL705960689US

PTO/SB/17 (12/99)
Approved for use through 09/30/2000. OMB 0651-0032
Patent and Trademark Office. U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

FEE TRANSMITTAL for FY 2000

Patent fees are subject to annual revision. Small Entity payments must be supported by a small entity statement, otherwise large entity fees must be paid. See Forms PTO/SB/09-12. See 37 C.F.R. §§ 1.27 and 1.28.

TOTAL AMOUNT OF PAYMENT ($) 816.00

Complete if Known	
Application Number	NOT YET ASSIGNED
Filing Date	CONCURRENTLY HEREWITH
First Named Inventor	Michael F. ANGELO et al.
Examiner Name	UNKNOWN
Group / Art Unit	UNKOWN
Attorney Docket No.	1662-28400 (P99-2550)

METHOD OF PAYMENT (check one)

1. ☑ The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:

Deposit Account Number: 03-2630

Deposit Account Name: Compaq Computer Corporation

☑ Charge Any Additional Fee Required Under 37 CFR §§ 1.16 and 1.17

2. ☐ **Payment Enclosed:** ☐ Check ☐ Money Order ☐ Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
101	690	201	345	Utility filing fee	690.00
106	310	206	155	Design filing fee	
107	480	207	240	Plant filing fee	
108	690	208	345	Reissue filing fee	
114	150	214	75	Provisional filing fee	

SUBTOTAL (1) ($) 690.00

2. EXTRA CLAIM FEES

			Extra Claims		Fee from below		Fee Paid
Total Claims	27	-20** =	7	X	18.00	=	126.00
Independent Claims	3	- 3** =	-0-	X	78.00	=	00.00
Multiple Dependent						=	00.00

**or number previously paid, if greater; For Reissues, see below

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
103	18	203	9	Claims in excess of 20
102	78	202	39	Independent claims in excess of 3
104	260	204	130	Multiple dependent claim, if not paid
109	78	209	39	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 126.00

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet.	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for reply within first month	
116	380	216	190	Extension for reply within second month	
117	870	217	435	Extension for reply within third month	
118	1,360	218	680	Extension for reply within fourth month	
128	1,850	228	925	Extension for reply within fifth month	
119	300	219	150	Notice of Appeal	
120	300	220	150	Filing a brief in support of an appeal	
121	260	221	130	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive - unavoidable	
141	1,210	241	605	Petition to revive - unintentional	
142	1,210	242	605	Utility issue fee (or reissue)	
143	430	243	215	Design issue fee	
144	580	244	290	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	
126	240	126	240	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	690	246	345	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	690	249	345	For each additional invention to be examined (37 CFR § 1.129(b))	

Other fee (specify) ____________

Other fee (specify) ____________

* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($)

SUBMITTED BY				Complete (if applicable)	
Name (Print/Type)	Marcella D. Watkins	Registration No. (Attorney/Agent)	36,962	Telephone	(713) 238-8000
Signature	Marcella D. Watkins			Date	September 29, 2000

WARNING:

Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Burden Hour Statement. This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

M:\C\1662\28400\PTO FEE TRANS 01

1662-28400
P99-2550

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR UNITED STATES LETTERS PATENT

FINGERPRINT VERIFICATION METHOD HAVING BAND DETECTION

By:

MICHAEL F. ANGELO
3303 Amber Forest Drive
Houston, Texas 77068
Citizenship: U.S.A.

MANUEL NOVOA
10110 Prospect Hill Drive
Houston, Texas 77064
Citizenship: U.S.A.

RICHARD CHURCHILL
8823 Edenbridge
Spring, Texas 77379
Citizenship: U.S.A.

FINGERPRINT VERIFICATION METHOD HAVING BAND DETECTION

BACKGROUND

The present invention generally relates to a method for preventing improper authentication in biometric devices. More specifically, the invention relates to a method of detecting and preventing latent-image attacks that take advantage of weaknesses in many existing fingerprint verification schemes.

Security is an issue for many modern transactions. As the world becomes increasingly interconnected and electronic commerce becomes more commonplace, so too does the need for security. Secret identifiers such as passwords and secret personal identification numbers (PINs) have become the normal security mechanism for people conducting transactions at automated teller machines, over the telephone, or over computer networks. While secret identifiers certainly provide a measure of security, they are problematic in that they depend on users memorizing the phrase, code word, security number, etc., for access to sensitive information. This situation is worsened by the proliferation of electronic accounts and transactions which typically force users into having a multitude of secret identifiers to keep track of. An attractive alternative to the use of secret identifiers is the use of biometric devices.

Biometric devices include devices that read, for example, fingerprints, retinas, or in some instances, detect voice characteristics. Biometric devices are advantageous for several reasons. Each of the above examples can detect traits that are unique to each individual, and which are largely impossible to forge. No memorization is required by the user to provide this "unique code". Further this "unique code" required to access the desired information is, for the most part, inseparable from the user, and hence is always available to the user when needed.

Fingerprint scanners have become one of the more common, commercially available biometric security devices. They operate on the principle that every person has fingerprint pattern that is unique to each person. The characteristics of these patterns may be compared to a previously-stored set of characteristics and, if a correlation exists, access is granted to the user.

The optical fingerprint verification scheme calls for the user to press the desired digit against a transparent surface. A scanner on the other side of the surface takes one or more pictures of the fingerprint pattern. The pattern is processed to identify its characteristics, and the characteristic are then compared to the previously-stored set of characteristics to determine if a match exists. Systems that implement this scheme are fairly inexpensive to mass-produce, and they are fairly robust at dealing with issues such as variable placement, orientation, pressure deformation, etc.. Nevertheless, they do suffer some potential weaknesses.

As with other biological characteristics, fingerprints in theory are very difficult to forge. As a practical matter, however, living people inevitably acquire a buildup of oils and residue on their skin. As objects are touched by fingers, some of this buildup is transferred from the ridges in our fingerprint patterns to the touched object, producing an image of the fingerprint pattern which is normally invisible. In the course of everyday life, people leave behind latent fingerprint images. If a person can lift one of these latent fingerprints, or recreate a valid fingerprint image from the latent image, and present it to the fingerprint recognition device, the device may recognize it and take a positive action. Just by using the systems as they were meant to be used, the user will normally leave a latent image of his fingerprint pattern on the transparent scanning surface.

One postulated method of attack on these systems involves lightly dusting the transparent surface with a fine powder. The fine powder will adhere to the oils left behind, but be easily removed from any areas where the oils are absent. When illuminated by an external light source,

the latent image becomes visible to the scanner. Since the pattern was created by the original fingerprint, the identified characteristics will match those on file, and access will be granted in the absence of any countermeasures. One solution to this type of attack requires users to carry a portable fingerprint platen that is to be placed onto the fingerprint scanner before use. Users then place their fingers on this portable platen. Once access is granted, the user removes the platen and keeps it and any latent fingerprint images with them. While this solution certainly reduces the danger of latent image access, it counteracts at least one of the advantages that fingerprint authorization seeks to offer. That is, it requires users to remember to carry the portable platen at all times.

In situations where portable platens are not a viable option or are not desired, countermeasures must be included in the verification method that will detect latent fingerprint image attacks. It has been recognized that scanners can distinguish real fingerprint patterns from latent or duplicate fingerprint patterns by capturing and comparing multiple images. A typical optical fingerprint scanner consists of a charge-coupled device (CCD) camera and an internal light source. The internal light will illuminate the fingerprint and the camera will capture the reflected image. A typical frame capture rate is on the order of about several dozen times per second. By comparing successive live images or groups of successive images, the scanner can determine if the image is changing. This countermeasure technique is effective because a live fingerprint image is constantly varying slightly due to changing pressure and motion caused by the user. On the other hand, a latent image remains constant because the latent image on the scanner surface is unchanged. Denying access for a static image thus stymies this attack.

However, it has been discovered that this countermeasure technique can be defeated if this postulated method of attack is augmented. If a strobe light is used to illuminate the static, latent

fingerprint image, the scanner can be induced to perceive differences between successive images. These image differences may be sufficient for the latent fingerprint image to be perceived as a real finger, and access may be improvidently granted. It is desirable, therefore, to provide a verification method with improved resistance to latent fingerprint image attacks.

BRIEF SUMMARY OF THE INVENTION

The problems noted above are solved in large part by a fingerprint verification method incorporating band detection. In one embodiment, the method includes capturing a fingerprint image and processing the image to determine if it includes bands attributable to changes in illumination intensity or some other attack during image capture. If such bands are detected, the method preferably aborts the creation of a fingerprint template. Otherwise, if this and other security screens are passed, the method preferably includes the creation of a fingerprint template which may be compared to a stored fingerprint template to verify user identity. If such verification is established, the user is granted access privileges. One embodiment of a system implementing this method includes a fingerprint scanner for capturing fingerprint images, and an interface card having a digital signal processor (DSP) or other suitable electronics for processing the fingerprint images and generating a fingerprint template representative of the images. The system may further include a general purpose computer coupled to the interface and configured to receive the fingerprint template. The general purpose computer can then use the fingerprint template to verify the identity of the user.

The improved recognition algorithm may advantageously preserve the convenience offered by a fingerprint scanning device while maintaining security and user confidence. The recognition

algorithm will also be adaptable to other biometric devices where latent images are a concern and is not limited to fingerprints scanners.

BRIEF DESCRIPTION OF THE DRAWINGS

For a detailed description of the preferred embodiments of the invention, reference will now be made to the accompanying drawings in which:

Fig. 1 shows a computer system having a biometric device;

Fig. 2 is a block diagram of the computer system in Fig. 1;

Fig. 3 is a block diagram of an interface card for a biometric device;

Fig. 4 is a flowchart of a verification method having band detection;

Fig. 5 shows a captured fingerprint image;

Fig. 6 shows the captured real fingerprint image with minutia information overlaid;

Fig. 7 shows a captured latent fingerprint image when illuminated by a strobe light;

Fig. 8 shows the captured latent fingerprint image with minutia information overlaid;

Fig. 9 is an exemplary histogram of grayscale values in a row of a real fingerprint image;

Fig. 10 is an exemplary histogram of grayscale values in a row of a latent fingerprint image when illuminated by an external light source;

Fig. 11 is an exemplary histogram of grayscale values in a row of a latent fingerprint image when not illuminated by an external light source;

Fig. 12 is an exemplary graph of the mode of the grayscale value histogram as a function of position along the Y-axis, for a real fingerprint;

Fig. 13 is an exemplary graph of the grayscale value histogram mode as a function of Y-axis position for a latent image illuminated by a steady external light source; and

Fig. 14 is an exemplary graph of the grayscale value histogram mode as a function of Y-axis position for a latent image illuminated by a strobe light.

NOTATION AND NOMENCLATURE

Certain terms are used throughout the following description and claims to refer to particular system components. As one skilled in the art will appreciate, computer companies may refer to a component by different names. This document does not intend to distinguish between components that differ in name but not function. In the following discussion and in the claims, the terms "including" and "comprising" are used in an open-ended fashion, and thus should be interpreted to mean "including, but not limited to…". Also, the term "couple" or "couples" is intended to mean either an indirect or direct electrical connection. Thus, if a first device couples to a second device, that connection may be through a direct electrical connection, or through an indirect electrical connection via other devices and connections.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Turning now to the figures, Fig. 1 shows an exemplary computer system in accordance with the preferred embodiment. The computer system of Fig. 1 includes a computer 12, a monitor 14, a keyboard 16, and a biometric device 18. Biometric device 18 is preferably a fingerprint scanner, but other biometric devices may also be employed. Although these components are shown separately here, they may be combined into one package such as, e.g. a laptop computer. The monitor 14, keyboard 16, and biometric device 18 are peripherals through which the user interacts with computer 12. As the computer 12 executes various software tasks, the user may be prompted via monitor 14 to take various actions such as entering a login command via keyboard 16 and

pressing a finger against the window on biometric device 18. The tasks executed by the computer 12 preferably include verifying the user's fingerprint and granting access to secured privileges.

Fig. 2 shows a block diagram of the exemplary computer system of Fig. 1. The computer system includes a CPU 102 coupled to a bridge logic device 106 via a CPU bus. The bridge logic device 106 is sometimes referred to as a "North bridge" for no other reason than it often is depicted at the upper end of a computer system drawing. The North bridge 106 also couples to a main memory array 104 by a memory bus, and may further couple to a graphics controller 108 via an accelerated graphics port (AGP) bus. The graphics controller 108 typically provides the video signal that drives monitor 14. The North bridge 106 couples CPU 102, memory 104, and graphics controller 108 to the other peripheral devices in the system through a primary expansion bus (BUS A) such as a PCI bus or an EISA bus. Various components that comply with the bus protocol of BUS A may reside on this bus, such as an audio device 114, a IEEE 1394 interface device 116, and a network interface card (NIC) 118. These components may be integrated onto the motherboard, as suggested by Fig. 2, or they may be plugged into expansion slots 110 that are connected to BUS A.

If other secondary expansion buses are provided in the computer system, as is typically the case, another bridge logic device 112 is used to couple the primary expansion bus (BUS A) to the secondary expansion bus (BUS B). This bridge logic 112 is sometimes referred to as a "South bridge" reflecting its location vis-à-vis the North bridge 106 in a typical computer system drawing. An example of such bridge logic is described in U.S. Patent No. 5,634,073, assigned to Compaq Computer Corporation. Various components that comply with the bus protocol of BUS B may reside on this bus, such as biometric device interface 122, hard disk controller 124, Flash ROM 126, and Super I/O controller 128. Additional slots 120 may also be provided for plug-in components that comply with the protocol of BUS B. The Super I/O controller 128 typically

interfaces to basic input/output devices such as a keyboard 132, a mouse 134, a floppy disk drive 130, a parallel port, a serial port, and sometimes various other input switches such as a power switch and a suspend switch.

The biometric device interface 122 couples to biometric device 18. The biometric device 18 typically includes little more than a window, an internal light source, and a camera. The electronics for powering and operating the biometric device 18 are included in the biometric device interface 122. As shown in Fig. 3, the interface 122 may include bus interface logic 302, a digital signal processor (DSP) 304, a power switch 306, and a memory 308. When software executed by CPU 102 initiates an identity verification procedure, the CPU 102 generates a fingerprint acquisition request which is received by the DSP 304 via the bus interface logic 302. The DSP 304 then closes switch 306 to power the biometric device 18 and executes a fingerprint acquisition procedure stored in memory 308. When powered, the biometric device 18 typically begins transmitting scanned image information at a rate of a few dozen frames per second.

A preferred fingerprint acquisition procedure 402 is given in Fig. 4. Beginning with block 404, the DSP 304 stores an image frame in memory 308. This image is preferably a grayscale image, but otherwise would appear somewhat like Fig. 5. In block 406, the DSP 308 processes the stored image to identify characteristic features of the fingerprint pattern. Among other things, this processing preferably includes the extraction of minutia from the fingerprint pattern.

The science of fingerprint identification has recognized that fingerprint patterns can be characterized by features such as ridge line endings and splits. The direction vector of the ridge line as it ends or splits may also be determined to provide greater security. These features are commonly termed "minutia". Fig. 6 shows an example of such extracted minutia, overlaid on the processed fingerprint pattern. The existence and relative positions (i.e. relative angles and relative

distances) of these features can be combined to form a "template" that differs from templates created from any other fingerprint patterns. More than one template may result from a given fingerprint pattern, but they correlate well with each other, and very poorly with templates from different fingerprint patterns. These templates offer other advantages, including greatly reduced storage requirements and the virtual impossibility of "reverse-engineering" a fingerprint that will correspond to the template.

Returning to Fig. 4, the DSP preferably captures a subsequent image frame in block 404 and repeats the feature extraction in block 406, repeating these steps until enough repetitions have been performed as decided in block 408. Then in block 410, the DSP compares the extracted features to determine if the series of image frames are duplicates. Because a real finger is expected to exhibit at least some minimal amount of variation across a series of frames, the detection of less than this amount of variation causes the DSP to abort the acquisition process and report failure in block 412. Otherwise, in block 414 the DSP checks for banding of one or more of the images.

Image banding is an indication of a latent-image strobe attack. The biometric device 18 typically scans and transmits images in a raster-fashion, i.e. one pixel row at a time in column order, with the rows transmitted in row order. If a latent image is dusted and illuminated with a strobe light at an appropriate frequency, the alternating illumination and non-illumination of the latent image will manifest as bands in the fingerprint image. Examples of appropriate frequencies may include those frequencies approximating the frame rate, or some integer multiple thereof (See, for example, Fig. 7), and those frequencies approximating the row scan rate, or some integer multiple thereof. Those pixels that are scanned while the strobe light is out will be dark with poor contrast. Those pixel rows that are scanned while the strobe light is illuminated will be much lighter with a generally improved image contrast. Unless the strobe light is exactly synchronized

with the frame rate, the bands will appear in different locations in subsequent frames. It is noted that the number and width of the bands may be independently varied by adjusting the frequency and duty cycle of the strobe light, and that similar effects may be obtained.

It is noted that image banding may also be an indication of other attack modes. For example, it is conceivable that some CCD cameras might be susceptible to induction (magnetic field) or electrical field attacks that induce similar banding effects to that of the latent-image strobe attack.

Fig. 8 shows the extracted minutia for the banded image. Note that some of the original minutia points were not identified in the areas obscured by the bands. As the bands move progressively in the series of frames, different minutia points will be "lost". This causes the extracted features to vary across the series of frames, allowing a latent-image to defeat the duplication test of block 410.

To detect image banding in block 414, some image analysis is needed. Fig. 9 shows an exemplary histogram of pixel values along one scanning row for a real fingerprint image (Fig. 5). Note that there are two well-defined peaks, with the larger peak representing the dark pixels and the smaller peak representing the light pixels. During periods of latent image illumination, the histogram changes to resemble that of Fig. 10. Two peaks are generally still visible, but the histogram has been skewed towards the light end. During periods when the strobe light is out, the histogram resembles that of Fig. 11. Nearly all the pixels are dark, and contrast is nearly non-existent.

The mode (highest peak) of the pixel row histogram can be used as an indication of the illumination level. Figs. 12-14 show the resulting relationship when this mode is plotted as a function of the row position. Fig. 12 shows the expected relationship for a real finger. Note that the

illumination level is relatively constant across the bulk of the finger, with some slight increase near the edges of the image. Fig. 13 shows the expected relationship for a latent image illuminated by a constant light source. The illumination level is generally higher and flatter than for a real finger. Fig. 14 shows the expected relationship for a latent image illuminated by a strobe light. The illumination level resembles that of Fig. 13, but drops dramatically in the banded regions.

In block 414, various techniques may be used to detect image banding. In the preferred embodiment, the DSP determines if excessive sudden variations in the grayscale mode exist. In another embodiment, the DSP tests for straight lines across the image having at least a predetermined width (e.g. two pixels). If bands are detected, the DSP aborts the acquisition process and reports failure in block 412. Otherwise, the DSP continues with the acquisition process, preferably performing additional tests such as a test for profile skew in block 416 and a test to see if the grayscale mode is relatively flat in block 418. These tests may each be performed on one or more captured images. Once the security screens have been satisfied, the extracted features are used to create a template in block 422. The DSP provides the template, encoded if desired, to the CPU. The CPU may then compare the template to a stored template, or may encode it and transmit it over a network for verification at some central facility. Once the CPU determines that a match exists, the CPU can then grant the user access. Note that for logging into a network, the template, encoded if desired, may be transmitted to a network login server which does the template comparison and grants access if a match is detected.

It is noted that the flowchart of Fig. 4 is for illustrative purposes only, and that the actual method used to provide security against latent image attacks may vary considerably from that discussed. Nevertheless, one of ordinary skill in the art will appreciate from this disclosure the

utility of detecting bands and various methods by which this detection may be accomplished. This disclosure is not intended to exclude such methods.

It is noted that the disclosed methods may, for example, be implemented in application specific hardware, or alternatively, software executing on a DSP or general purpose CPU. It is not intended to limit the implementation to the specific embodiment described above.

The above discussion is meant to be illustrative of the principles and various embodiments of the present invention. Numerous variations and modifications will become apparent to those skilled in the art once the above disclosure is fully appreciated. Testing for the existence of bands in the image may be performed in a wide variety of ways. For example, bands may be determined to exist only if the position of the excessive mode variances change position from frame to frame. This might prevent an artifact such as a scar from triggering a false detection of a band. Spatial Fourier transforms may be performed to determine changes in spectral properties that might indicate the presence of bands. It is intended that the following claims be interpreted to embrace these and other band detection methods and variations and modifications thereof.

CLAIMS

What is claimed is:

1. A computer system, comprising:

a biometric device configured to transmit images;

an interface coupled to the device to receive the transmitted images, wherein the interface is configured to determine if the transmitted images include bands.

2. The computer system of claim 1, wherein the interface is configured to report failure if the interface determines that the transmitted images include bands.

3. The computer system of claim 1, wherein the bands are attributable to illumination changes.

4. The computer system of claim 1, wherein the bands are attributable to electrical changes.

5. The computer system of claim 1, wherein the bands are attributable to induction across the biometric device.

6. The computer system of claim 1, wherein the interface is configured to process the images to determine minutia information.

7. The computer system of claim 6, wherein the interface is configured to convert the minutia information into a template only if the interface does not determine that the transmitted images include bands.

8. The computer system of claim 1, wherein the biometric device is a fingerprint scanner configured to transmit images of fingerprints.

9. The computer system of claim 1, wherein the interface determines if one or more of the transmitted images include at least one straight line having at least a predetermined width across the image.

10. The computer system of claim 1, wherein the interface processes a plurality of rows to determine a corresponding plurality of grayscale value histograms.

11. The computer system of claim 10, wherein the interface processes the plurality of grayscale value histograms to determine a corresponding plurality of modes for the grayscale value histograms.

12. The computer system of claim 11, wherein the interface determines if the plurality of modes indicate the existence of bands in the images by determining if the modes exhibit variations greater than a predetermined amount.

13. The computer system of claim 1, wherein the interface connects to an expansion slot, and wherein the computer system further comprises:

a system memory configured to store software;

a processor coupled to the system memory and configured to execute the software, wherein the processor is further coupled to the interface, wherein the software configures the processor to initiate operation of the interface and biometric device.

14. The computer system of claim 13, wherein the processor is configured to receive a template from the interface, and wherein the processor is configured to compare the template to a stored template.

15. The computer system of claim 13, wherein the computer system further comprises:

a network interface coupled to a network login server, wherein the network login server is configured to receive a template from the interface, and wherein the network login server is configured to compare the template to a stored template.

16. A fingerprint verification method that comprises:

capturing a fingerprint image; and

determining if the fingerprint image includes bands, and if so, aborting creation of a fingerprint template.

17. The method of claim 16, wherein said bands are bands attributable to illumination changes.

18. The method of claim 16, wherein the determining is one of a plurality of security tests, and wherein the method further comprises:

creating a fingerprint template if the image passes the plurality of security tests.

19. The method of claim 18, wherein the creating includes:

extracting minutia information from the fingerprint image; and

converting the minutia information into the fingerprint template.

20. The method of claim 19, wherein the plurality of security tests includes:

determining if minutia information from one fingerprint image matches minutia information from another fingerprint image.

21. The method of claim 16, wherein the capturing includes:

illuminating a window from a scanning side;

scanning light reflected back through the window in raster fashion.

22. The method of claim 16, wherein the determining includes:

detecting at least one straight line spanning the image and having at least a predetermined width .

23. The method of claim 16, wherein the determining includes:

finding a grayscale value histogram mode for each row of the fingerprint image;

calculating a variance of the modes; and

determining that the fingerprint image includes bands if the variance exceeds a predetermined threshold.

24. The method of claim 18, wherein the plurality of tests includes: and

extracting minutia information from a plurality of fingerprint images;

comparing the minutia information of the plurality of images to determine if at least a minimum amount of variation exists, and if not, aborting the creation of the fingerprint match template.

25. A fingerprint verification system that comprises:

a capture means for capturing a fingerprint image; and

a processing means for determining if the fingerprint image includes bands attributable to condition changes during the capturing of the fingerprint image.

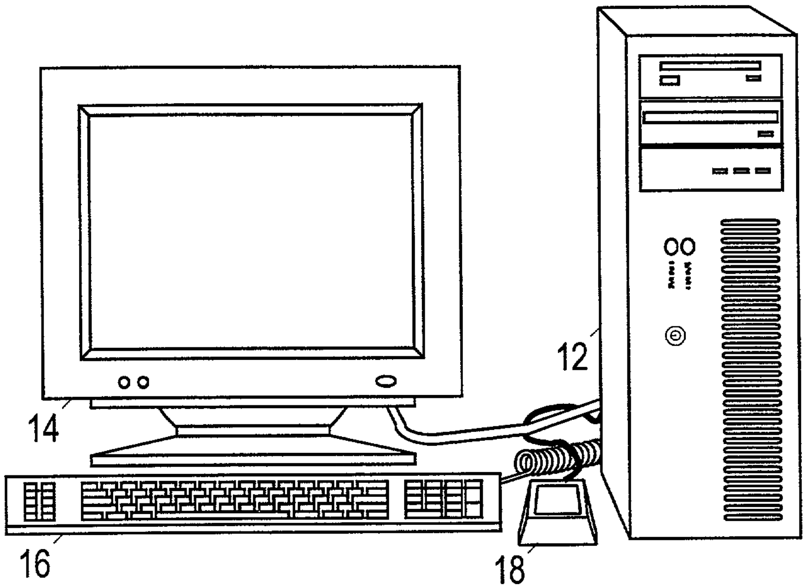
26. The system of claim 25, wherein said condition changes include illumination intensity changes.

27. The system of claim 25, wherein if the processing means determines that the fingerprint image includes bands, the processing means prevents creation of a fingerprint template from information in the fingerprint image.

ABSTRACT

A fingerprint verification method having band detection is provided. In one embodiment, the method includes capturing a fingerprint image and processing the image to determine if it includes bands attributable to changes in illumination intensity during image capture. If such bands are detected, the method preferably aborts the creation of a fingerprint template. Otherwise, if this and other security screens are passed, the method preferably includes the creation of a fingerprint template which may be compared to a stored fingerprint template to verify user identity. If such verification is established, the user is granted access privileges. One embodiment of a system implementing this method includes a fingerprint scanner for capturing fingerprint images, and an interface card having a digital signal processor (DSP) or other suitable mechanisms including software or electronics for processing the fingerprint images and generating a fingerprint template representative of the images. The system may further include a general purpose computer coupled to the interface and configured to receive the fingerprint template. The general purpose computer can then use the fingerprint template to verify the identity of the user.

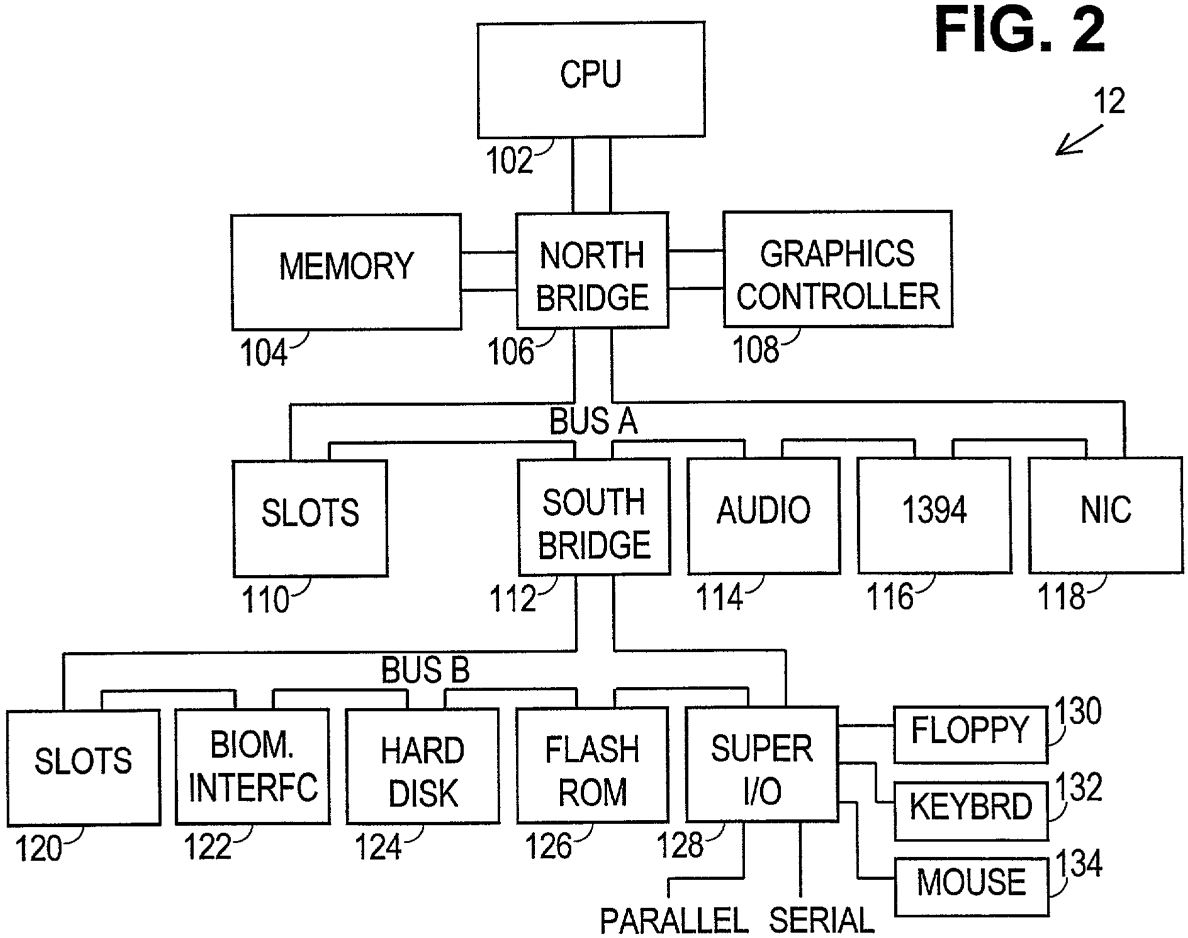
DJK
#26602 v2 - CPQ284PAT·



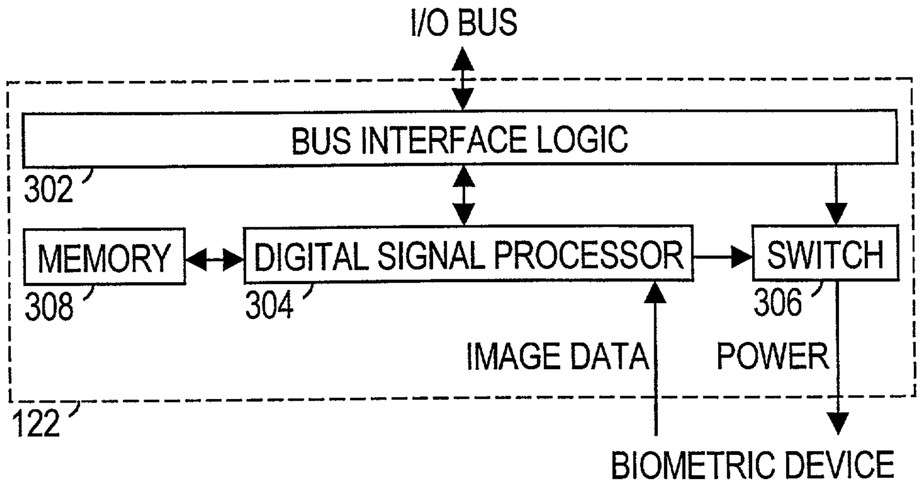
12
14
16
18

FIG. 1

FIG. 2

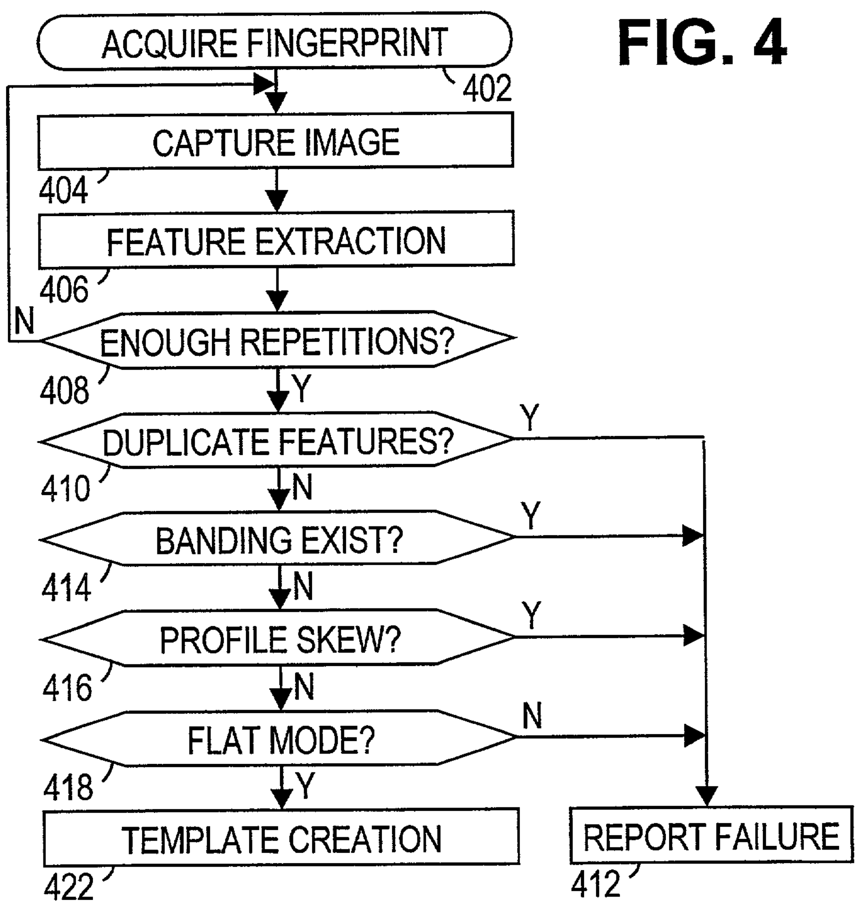


12
CPU
102
MEMORY
104
NORTH BRIDGE
106
GRAPHICS CONTROLLER
108
BUS A
SLOTS
110
SOUTH BRIDGE
112
AUDIO
114
1394
116
NIC
118
BUS B
SLOTS
120
BIOM. INTERFC
122
HARD DISK
124
FLASH ROM
126
SUPER I/O
128
FLOPPY
130
KEYBRD
132
MOUSE
134
PARALLEL
SERIAL



I/O BUS
BUS INTERFACE LOGIC
302
MEMORY
DIGITAL SIGNAL PROCESSOR
SWITCH
308
304
306
IMAGE DATA
POWER
122
BIOMETRIC DEVICE

FIG. 3



ACQUIRE FINGERPRINT
402
CAPTURE IMAGE
404
FEATURE EXTRACTION
406
N
ENOUGH REPETITIONS?
408
Y
DUPLICATE FEATURES?
Y
410
N
BANDING EXIST?
Y
414
N
PROFILE SKEW?
Y
416
N
FLAT MODE?
N
418
Y
TEMPLATE CREATION
422
REPORT FAILURE
412

FIG. 4

FIG. 5

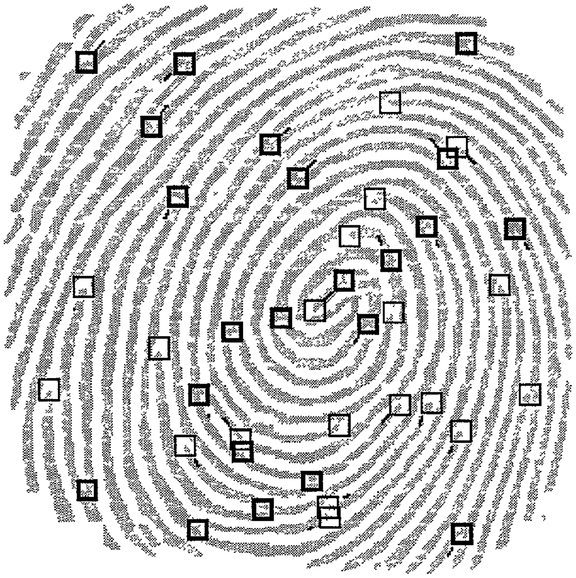


FIG. 6

FIG. 7

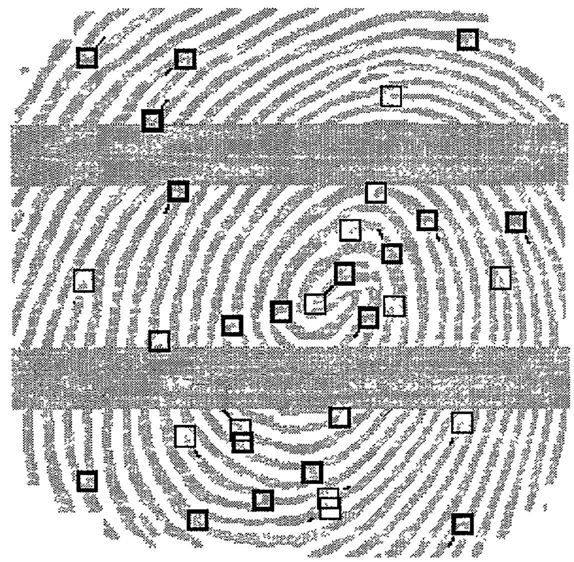


FIG. 8

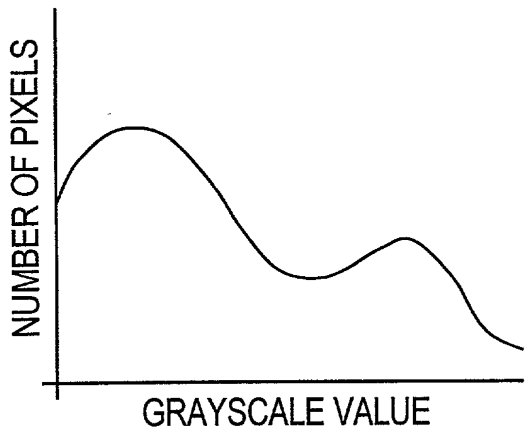


FIG. 9

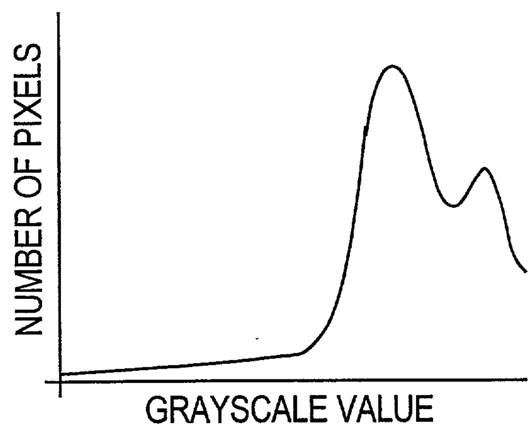


FIG. 10

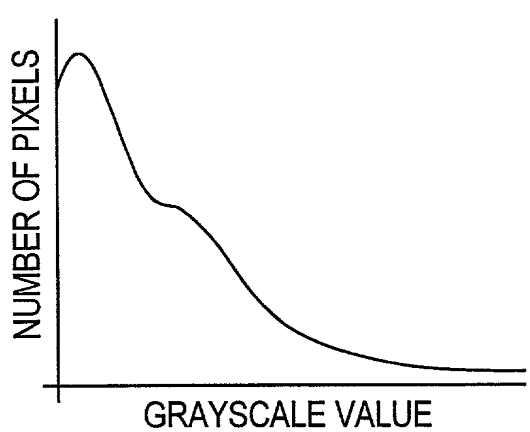


FIG. 11

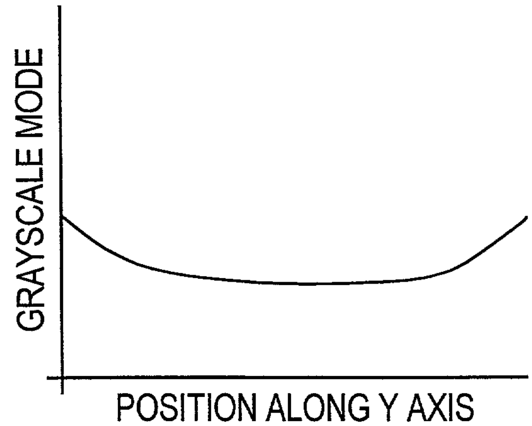


FIG. 12

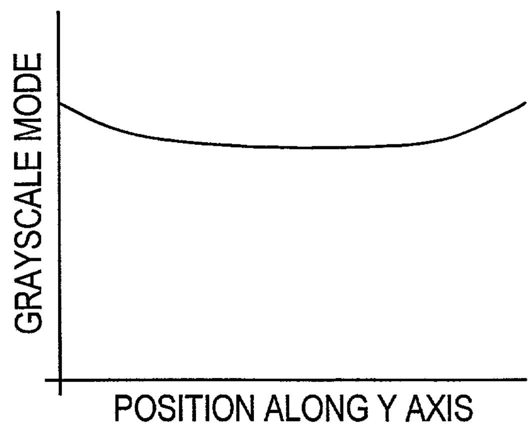


FIG. 13

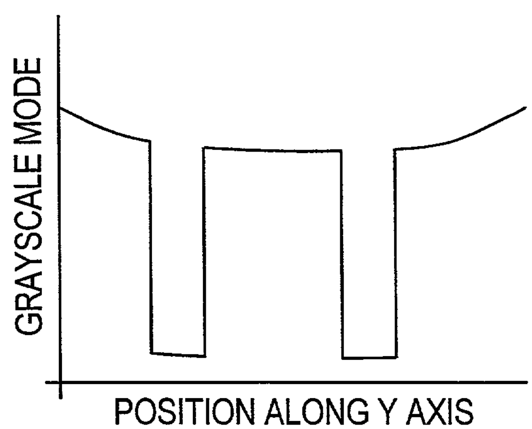


FIG. 14